THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 9 NUMBER 11
AND HOMELAND SECURITY

MAY 2011
DEFENSE INDUSTRIAL BASE SECTOR

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz
Shahin Saloom

JMU COORDINATORS
Ken Newbold
John Noftsinger

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

This month's issue of *The CIP Report* highlights the Defense Industrial Base (DIB) Sector. This Sector is responsible for providing the products and services essential to mobilizing and sustaining this Nation's military operations.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, representatives from the Defense Industrial Base Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) provide an overview of the DIB Sector. Next, a Senior Policy Analyst for National Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of theKathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation discusses the current status of the DIB Sector. The National Defense Industrial Association (NDIA), in a previously published policy/issue paper, then expounds upon four main themes that need to be addressed to sustain a successful manufacturing policy within the DIB Sector.

This month's *Legal Insights* describes and evaluates the recent decision of the Unites States Air Force (USAF) to award the Boeing Company the task of developing new air refueling tankers.

We also include a "Save the Date" for the 5th Annual Security Analysis and Risk Management Association (SARMA) Conference. The theme of the conference is "Security Risk 10 Years After 9/11: How Far Have We Come and What Lies Ahead?" Finally, there is an announcement for the 20th Annual GIS for Oil and Gas Pipeline Conference as well as a reminder about the 10th Workshop on Economics of Information Security (WEIS) and the Workshop on Cybersecurity Incentives (WoCI).

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

The Defense Industrial Base Sector

by Charles Kosak, Acting Deputy Assistant Secretary of Defense for Homeland Defense Strategy, Force Planning and Mission Assurance, Chair — Defense Industrial Base Government Coordinating Council, U.S. Department of Defense, and
Major General Barry Bates, USA (ret), Chair — Defense Industrial Base Sector Coordinating Council, National Defense Industrial Association

Defense Industrial Base Sector Overview

Critical infrastructure and key resources (CIKR) are essential to the Nation's security, economic vitality, and way of life. Accordingly, national policy objectives require Federal departments and agencies to identify and prioritize CIKR, to enhance CIKR protection against attacks, and to strengthen resilience for a range of manmade or national hazards. Recognizing that each critical infrastructure sector possesses its own unique characteristics, operating models, and risk landscapes, national policy also designates a Sector-Specific Agency (SSA) to oversee each of the 18 national infrastructure sectors. The Department of Defense (DoD) is the SSA for the Defense Industrial Base (DIB) Sector and leads a collaborative, coordinated effort to identify, assess, and improve risk management of critical infrastructure within DIB. The DIB Sector's vision is to collaboratively eliminate or mitigate unacceptable levels of risk to physical, human, and cyber assets, thus ensuring that DoD continues to fulfill its mission; and that DIB activities continue to effectively support national security objectives, public health and safety, and public confidence.

DIB is defined as the worldwide industrial network with capabilities to perform research and development, and to produce, deliver, and maintain military weapon systems, subsystems, or components. It is composed of hundreds of thousands of worldwide government and private sector sites, with the majority of them being privately owned. DIB companies can range from small proprietors to Fortune 500 corporations employing tens of thousands of people. Contrary to common belief, DIB does not include commercial infrastructure, such as power or other utilities. These commercial infrastructures are addressed by other SSAs. Defense-related products and services provided by DIB equip, inform, mobilize, deploy, and sustain forces conducting global military and humanitarian operations. DIB companies are subdivided into segments and sub-segments that produce weapon system platforms, components, and expendables. This categorization is used by DoD to classify the contributions of particular DIB assets, as well as to analyze the criticality of the assets within the Sector. Figure 1 (on page 3) outlines those segments.

Key Collaborative Forums

Effectively executing SSA responsibilities requires significant collaboration between the various DoD organizations that have DIB responsibilities, industry partners, and other Federal departments and agencies. Many DoD organizations have responsibilities that support national CIKR protection objectives. Implementing national SSA responsibilities requires significant coordination across DoD components. Policy and DoD roles and responsibilities for critical infrastructure are included in DoD Directive 3020.40, available at: http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf.

Voluntary partnership is a central tenet of national efforts to build more secure and resilient U.S. infrastructure and to DoD's efforts to identify, assess, and improve DIB resilience. To implement its SSA responsibilities, DoD uses several key forums:

- **DIB Government Coordinating Council (GCC):**
We partner with 6 Federal Departments that have equities

(Continued on Page 3)

Sector Overview *(Cont. from 2)*

impacting DIB. These include the Departments of State, Treasury, Justice, Commerce, Homeland Security, and most recently, the Department of Energy.

• **DIB Sector Coordinating Council (SCC):** The DIB SCC is chartered as the framework enabling DIB private sector owners and operators to engage DoD, the Department of Homeland Security (DHS) and SSA on matters related to CIKR resilience. Six defense industry associations and 22 companies make up the DIB SCC.

• **DIB Joint Coordinating Council Meetings:** The GCC, SCC, and select subject matter experts meet quarterly to discuss and resolve joint efforts related to DIB. These meetings are conducted under the DHS Critical Infrastructure Public Advisory Council (CIPAC) framework to allow for a free exchange of information between industry and government on critical issues.

• **DIB Critical Infrastructure Protection Conference (DIB CIP):** An annual conference co-sponsored by the National Defense Industrial Association (NDIA) and DoD that addresses security and resilience of the Sector. The 2011 theme is "DIB CIP 2020: Setting the Vision & Strategy for the Next Decade." Senior level speakers and panelists will address core topics such as: Managing Risks, DIB Cyber Mission Assurance, Infrastructure Dependencies, Information Sharing, Preparedness Resiliency and Response, Recovery and Reconstitution. For more information on the postponed 2011 DIB CIP Conference, please visit the NDIA website at: http://www.ndia.org/meetings/1030/Pages/default.aspx.

Figure 1: DIB Segments and Sub-segments

AIRCRAFT	Fixed Wing	C4I	Strategic C4
	Helicopter		Tactical C4
	Unmanned Aerial System		Night Vision/Infrared
SHIPBUILDING	Surface Ship		Electronic Warfare
	Sub Surface Ships		Ground Stations/Data Links
	Unmanned Underwater System		Navigation Systems
AMMUNITION	Ammunition (Large Caliber)		Signal Warfare
	Ammunition (Medium caliber)	GROUND VEHICLES	Tracked Vehicles
	Ammunition (Small Caliber)		Wheeled Vehicles
	Artillery	SOLDIER SYSTEMS	Troop Support
	Bombs/Bomb Accessories		Chem Bio Defense (various)
	Dispenser Munitions	MISSILE	Precision Guided Munitions
	Flares		Strategic
	Grenades		Tactical
	Mines	SPACE	Satellite
	Mortars		Launch Vehicle
	Rockets & Warheads		Ground Stations
ARMAMENTS	Cannon		
	Man Portable		
	Mounted		

• **Enduring Security Framework (ESF):** The ESF is a public-private forum of senior leaders in both industry and government focused on information and communication technology matters, including cybersecurity and other information assurance threats. The Executive Council includes the Deputy Secretary of Defense, the Deputy Secretary of Homeland Security, the Director of National Intelligence, and Chief Executive Officer (CEO) level industry executives. The operations working group focuses on DIB issues and brings industry and government together to mitigate emerging and current cyber-based threats to DIB and associated technology bases. DIB GCC and SCC leaders participate in this forum.

DIB Roles and Responsibilities

Many DoD organizations have responsibilities that support national CIKR protection objectives. Implementing national SSA responsibilities requires significant coordination across DoD components. Table 1 (see page 5) outlines some of the key DoD players and their primary DIB roles.

Joint Objectives

Under the leadership of the combined Government and Sector Coordinating Councils, the DIB Sector developed a Joint Business Plan (JBP) to focus annual activity on a set of shared objectives. These objectives are based on the goals of the DIB Sector Specific Plan and on current trends or threats that impact DIB. This joint plan identifies concrete and action-oriented

(Continued on Page 4)

Sector Overview *(Cont. from 3)*

objectives with assigned timelines and responsible leads. The JBP reenergized DoD and private sector engagement within the national CIKR protection framework and set about making concrete progress for resilience functions throughout the Sector. The 2010 JBP has 22 objectives organized into five focus areas: Criticality, Threat Comprehension, Dependency Analysis, Assessments, and Information Sharing.

Criticality: DoD oversees the annual process that determines the criticality of private sector DIB assets vital to DoD missions. Annually, DoD civilian and service components nominate assets that meet these criteria to identify important or critical capabilities necessary to maintain DoD missions. This year, for the first time, our industry partners will also be engaged in this critical asset identification and prioritization process. DoD recognized that the DIB SCC has valuable knowledge of industry capabilities, supply chains, dependencies, and vulnerabilities that could help shape the annual critical asset list.

Threat Comprehension: DoD is working to address several key threats identified as DIB priorities, including cyber threats, insider threats, and front companies. DIA's Joint Intelligence Task Force — Counter Terrorism (JITF-CT) now provides periodic classified threat briefings on topics of interest to DIB SCC partners. The true success of these roundtable discussions is the resulting relationship and trust building between the intelligence community and the private sector.

Dependency Analysis: Understanding DIB dependency on other critical infrastructure sectors is vital to DoD's ability to engage in interagency process and to advocate for risk management of those dependencies. The Department is analyzing existing assessment data to identify DIB energy dependency trends to provide DIB partners a baseline for analyzing their facilities. Additionally, DoD will undertake two regional energy dependency assessments by the end of the fiscal year and provide a dependency methodology for use by DIB partners.

Assessments: DIB critical assets are currently assessed by various DoD components and other Federal agencies. The companies themselves also identify risk and validate security, functionality, and resilience. DoD is examining ways to streamline DIB assessments and share assessment results more widely among organizations with DIB responsibilities. One key initiative is an agreement between DHS and DoD that will begin more focused joint assessments of DIB facilities and allow the two organizations to share the data gathered from past and future assessments.

The SCC plans to implement physical security, cybersecurity, and resilience self-assessment tools that will produce a relative score for each facility and allow DoD and DHS to focus assessment efforts. A concise DIB Sector physical security self-assessment tool has been designed for small and medium size companies and is available to DIB companies on the Homeland Security Information Network (HSIN) DIB portal.

Information Sharing: A significant issue of concern is increasing information sharing capabilities, mechanisms, and practices with DIB. Both industry and government partners identified their information sharing requirements as a baseline for future initiatives.

A first step to improve information sharing was recently completed by DHS and the DIB SCC by developing and deploying a private sector portal on the HSIN. This tool enables CIKR owners and operators to access threats, warnings, and risk information. It also allows them to participate in discussions, awareness webinars, and other types of collaboration. To request access to the HSIN-DIB portal, private sector companies should submit their name, title/position, company, or organization and work email address to cikriseaccess@dhs.gov.

DoD has identified existing information sharing portals and is pursuing the national goal of a federated set of authoritative portals that allow industry stakeholders to visit one site for all of their information sharing needs. DoD is also pursuing a system to host a robust two-way information sharing mechanism at the classified level. DoD recently implemented an emergency notification system that can reach DIB SCC partners, and will be expanded over time to the

(Continued on Page 5)

Sector Overview *(Cont. from 4)*

Table 1: DoD Component DIB Roles and Responsibilities	
DoD Component	**Responsibilities**
Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))	AT&L sets industrial policy and manages the multi-billion dollar procurement process, including the customer- vendor relationship with industry. AT&L is responsible annually for development and documentation of privately held DIB assets that are critical to maintaining DoD missions.
Under Secretary of Defense (Intelligence) (USD(I))	USDI frames policy and oversees intelligence, counterintelligence, and security support, as appropriate, to the national DIB Sector. This includes establishing national DIB Sector intelligence requirements that are reflected in Combatant Command, the Services, DoD, and national collection plans. USDI also manages industrial security policy, which establishes the requirements for cleared DIB members to safeguard classified information in their possession while performing work on contracts, programs, bids, or research and development efforts.
Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs (ASD(HD&ASA))	The Secretary of Defense delegated SSA responsibilities for the DIB to Under Secretary of Defense for Policy. HD&ASA under the USD(P) develops DoD policy, productive partnerships, and strategies to enhance the security and resilience of the DIB in coordination with National CIKR policy objectives. HD&ASA leads key DIB collaboration forums and is responsible for overall critical infrastructure policy development within DoD.
Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))	ASD (NII) implements the Defense Industrial Base Cyber Security/Information Assurance (DIB CS/IA) pilot, which was established in 2007 by the Deputy Secretary of Defense with the support of an initial small group of DIB Chief Executive Officers (CEOs). The mission of this program is to improve protection of critical DoD unclassified program and technology information residing on, or transiting, DIB unclassified systems and networks. This collaborative information assurance program involves cyber threat information sharing, incident reporting and remediation, and intrusion assessments of compromised data. Based on lessons learned and with procedures in place, the DIB CS/IA program is transitioning from a pilot status to a full program that will allow participation by all qualified defense contractors. The qualifications will be in an Interim Final Rule published in the Federal Register, date to be determined (expected Summer 2011). Planning is also underway for a follow-on pilot with non-cleared defense contractors.

(Continued on Page 6)

Sector Overview *(Cont. from 5)*

Table 1: DoD Component DIB Roles and Responsibilities	
DoD Component	**Responsibilities**
Deputy Assistant Secretary of Defense for Cyber Policy	Develops DoD strategy and policy for operations in cyberspace. Responsible for the oversight of DoD cybersecurity activities in support of the DIB and the other agencies of the U.S. Government.
Defense Contract Management Agency (DCMA)	DCMA's Industrial Analysis Center (IAC) manages the relationship with the DIB through their Contract Management Offices. The Homeland Defense division performs mission-focused vulnerability assessments on DIB assets. IAC also provides trend analysis related to DIB resiliency, analyzes mission impact during DIB incidents, manages the annual criticality identification process, and identifies DIB resiliency initiatives.
Defense Security Service (DSS)	DSS is a member of the DIB GCC and is responsible for securing the Nation's technological base and overseeing the protection of U.S. and foreign classified information in the hands of industry. DSS also clears industrial facilities, personnel, and associated information systems, which includes security inspections; collects, analyzes and provides threat information to industry and government partners; provides advice to industry; delivers security education and training, and provides information technology services that support the industrial security mission of DoD and its partner agencies.
Military Services	Each of the Services maintains acquisition and security relationships with DIB members. The Services conduct vulnerability assessments and are a key voice in determining critical DIB assets. They manage the risk of loss or degradation of critical infrastructure and incorporate defense critical infrastructure into education, outreach and training programs, including the testing and exercising of mitigation and response plans.
The National Guard	The National Guard supports the organization and training of DIB vulnerability assessment teams in collaboration with DCMA.

Table 1: DoD Component DIB Roles and Responsibilities

(Continued on Page 18)

U.S. Defense Industrial Base at a Turning Point

by Mackenzie Eaglen*
Heritage Foundation

Last year, the Obama Administration, Secretary of Defense, and Congress began reshaping the U.S. military by changing the direction of defense investments and canceling programs with a total lifetime value of over $300 billion (if seen through completion). The list of defense cuts include a combat search and rescue helicopter; the F-22 fifth generation fighter; the Army's future combat systems (primarily a ground vehicle program); the multiple-kill vehicle for missile defense; a bomber for the Air Force; the VH-71 presidential helicopter; a transformational satellite program; and the second airborne laser aircraft. In addition, the Administration decided to extend the construction of an aircraft carrier by an extra year from four to five, reduce the number of ground-based midcourse defense interceptors from 44 to 30, and indefinitely delay the Navy's next generation cruiser.

Furthermore, the current Fiscal Year 2011 defense budget is not being spared the axe. Some of the planned reductions include ending production of the country's only wide-bodied cargo aircraft, the C-17; terminating the EPX intelligence aircraft; permanently canceling the Navy's cruiser; ending another satellite program; and killing the expeditionary fighting vehicle program for the Marine Corps. The Army's surface-to-air missile program and its non-line-of-sight cannon are also slated to end. The Marine Corps now has its version of the Joint Strike Fighter on probation.

Some of these cancelations, including the presidential helicopter, next generation bomber, the Army's combat fighting vehicle, and the Marine Corps' amphibious assault vehicle will be resurrected in future defense budgets because the need for them has not gone away. These program cancelations or deferrals should be taken in context. Of the roughly $400 billion the DoD spends on goods and services per year, over half of that amount goes to service contracts, not equipment. The cuts to major manufacturing production lines and the defense industrial base are significant, since one in ten American manufacturing jobs is in the defense industry.[1]

Additionally, the defense spending outlook for the coming years shows defense budgets declining in real terms. As part of Washington's efforts to "reduce enormous budget deficits, other defense accounts (from the base or 'peacetime' budget) might decline by 5 to 10 percent given the most current ideas and plausible projections now available. Taken together, these two effects could reduce funds directed to American defense companies by well over $100 billion a year, or at least one third."[2]

Aerospace, Shipbuilding, and Defense Workforce Shrinking

America's defense manufacturing industrial base continues to shrink because of defense investment decisions over the past two decades and is accelerating due to budget decisions approved the past two years. This is worrisome on a policy level but also on a practical level. Many of these significant changes are being made in the absence of any careful evaluation of America's global mission. This could lead to hollow security commitments around the world or, worse, a modern-day hollow force.

(Continued on Page 8)

[1] Charley Keyes, "Defense Industry Braces for Shutdown," CNN, April 7, 2011 at http://money.cnn.com/2011/04/07/news/economy/defense_contractors_shutdown/index.htm.

[2] Michael O'Hanlon, "The National Security Industrial Base: A Crucial Asset of the United States, Whose Future May be in Jeopardy," The Brookings Institution, February 2011, p. 4, at http://www.brookings.edu/~/media/Files/rc/papers/2011/02_defense_ohanlon/02_defense_ohanlon.pdf.

DIB Challenges *(Cont. from 7)*

The U.S. military relies heavily upon the highly-skilled workforce to build the most cutting-edge systems that have given the United States its technical overmatch against our enemies for decades. The workforce hourly wage in aerospace and defense leads all industry sectors, including technology and government. The combined effects of a shrinking workforce and the graying of this industry are problems without clear solutions identified or agreed upon by policymakers.

Over the last decade, the aerospace and defense workforce fell from over one million to 600,000 people. In the past two years, since the latest round of modernization cuts began, over 40,000 direct aerospace and defense jobs have been lost. In reality, this number is much higher (by a factor of three) because of the effect on the second and the third tier jobs that support production line workers. Furthermore, the challenge posed by the aging of the defense industrial base is now growing beyond designers and engineers to include highly-skilled assembly line workers.

These trends are even more troubling when considering that the aerospace industry is a net export leader for the United States. Indeed, several major defense lines are sustained only through foreign military sales. The number of such lines is growing as the number of "new start" U.S. major programs decline. For the first time in the history of aviation (100 years), the United States has no manned commercial or military aircraft under design. Policymakers face the challenge of how to sustain the military's technological edge as the number of defense programs decline qualitatively and quantitatively. Expertise in this industry builds slowly. Once highly-skilled workers exit the Federal workforce, they are difficult to recruit back and more expensive to retrain.

The size and talent of the defense industrial base will continue to shrink. This will reduce contractor competition that helps save taxpayer money and spurs additional innovation in unique military technologies. A loss of innovation and an increase in uncertainty facing the companies, vendors, and suppliers that comprise this critical workforce will put this national asset at risk.

How to Reverse the Decline

Continuous replacement of military platforms is vital to ensuring a superior fighting force. In less than ten years, the number of major defense contractors has fallen from fifty to six. Ten years ago, America boasted six major aircraft producers, while today we have only two. Securing America's military dominance for the decades ahead will require:

- An industrial base that can retain a highly-skilled workforce with critical skill sets, and

- Sustained investment in platforms that offer future commanders and civilian leaders a vital set of core military capabilities and equipment to respond to any threat.

In order to properly guide future defense investments, an industrial policy must include substantial input from defense acquisition leaders, program managers, systems engineers, compliance managers, auditors, and other experts. Defense leaders should also constantly assess the health of the defense supply chain. The next national defense strategy should discuss in detail the ability of the industrial base to respond rapidly to the changes in strategic environment.

Specialized design, engineering, and manufacturing skills are the critical workforce ingredients in sustaining an industrial base capable of building next-generation systems. Already at a turning point, the potential closure of major defense manufacturing lines in the next five years with no additional scheduled production could shrink this national asset even further. While the manufacturing workforce alone should not dictate acquisition decisions, the potential "brain drain" must be considered when Congress determines whether or not to permanently shut down major production lines — particularly shipbuilding and aerospace.

Congress should broadly support increase in foreign military sales between the United States and its allies and partner nations. America's defense industrial base serves an important role in building the military capacity of foreign allies and enhancing their interoperability with the U.S. military. These efforts

(Continued on Page 20)

National Defense Industrial Association Position Paper on the Defense Industrial Base

by National Defense Industrial Association (NDIA)

This article is the condensed version of a previously published position/issue paper written for the current edition of NDIA's Top Issues for 2011. For full access to this paper, please click here.

America's military strength remains vital to preserving the Nation's interests and sustaining international stability. While much of this strength is derived from the professionalism and skills of America's armed forces, the technologically superior military platforms developed and produced by the U.S. defense industrial base have been vital to ensuring a superior fighting force. In both peace and war, America's defense manufacturing industrial base has allowed the United States to meet the full spectrum of missions the military has been called upon to fulfill. Securing America's military dominance for the decades ahead will require an industrial base that can retain a highly-skilled workforce with critical skill sets and sustained investment in platforms to respond to any potential threat.

U.S. national security depends heavily upon our domestic manufacturing capabilities and DoD relies upon the U.S. defense industrial base for leap-ahead, innovative technologies with which to equip our warfighters. It is critical to understand that in the defense sector, if the government does not fund a particular system, industry will abandon the effort, including the underlying industrial capabilities. Work force and resources will move on to other funded programs. The segment that is not funded will eventually wither and industry will lose that capability. Once lost, these domestic capabilities take substantially more time and funding to regain. The U.S. industrial base is in crisis and needs attention, and based upon several key studies, the U.S. defense industrial base is facing a similar and parallel crisis. Moreover, the current government procurement policies will not produce the competitive, responsive, efficient, and innovative industrial base that is required to face these challenges.

There are four main themes that need to be addressed to sustain a successful manufacturing policy: leadership and cultural perceptions; research and development (R&D) in manufacturing; strategic manufacturing capabilities for national security; and workforce and infrastructure.

Leadership and the Cultural Perceptions

The health of the defense industrial base has to be elevated to a higher level in the scope of U.S. policy considerations. This requires active and senior leadership, both within the Administration and DoD. The U.S. agriculture sector represents one percent of our Gross Domestic Product (GDP), employs 1percent of the workforce, and is represented by a cabinet Secretary. The manufacturing sector is ten times larger and is represented by an Assistant Secretary for Manufacturing and Services within the International Trade Administration of the Department of Commerce. Manufacturing and the industrial base are important enough for representation by at least a Deputy Secretary, which would also raise the level of coordination between government agencies.

In turn, defense manufacturing issues need more senior leadership within DoD to unite policy, strategy, investment, and implementation. Currently, DoD has a Director for Industrial Policy, with responsibility for stimulating competition and sustaining industrial capabilities within the defense industrial base. This office monitors the industrial base and uses established authorities to promote competition or defense priorities over commercial production such as the Defense Production Act.[1] However, DoD requires senior leadership for

(Continued on Page 10)

[1] Public Law 81-774 enacted on September 8, 1950, in response to the start of the Korean War.

NDIA *(Cont. from 9)*

manufacturing which has the authority to define strategy and set policy, but also implement R&D alignment, infrastructure revitalization, and workforce investment across all of DoD. There is also a problem in the United States with the perception of manufacturing. In a recent survey by the Manufacturing Institute and Deloitte, 81percent of respondents believe that America's manufacturing base is either important or very important to their standard of living and to economic prosperity, and 77 percent think the United States needs a more strategic approach to the development of its manufacturing base. However, only 30 percent of respondents would encourage their children to pursue a manufacturing career. The perception is that manufacturing is something akin to an iron foundry in the year 1900, but the reality is a manufacturing workforce is as likely to use a keyboard as a wrench, and operates in a clean, safe environment. The government needs to change this outdated perception in order to get the high-caliber workforce needed for high-tech manufacturing, particularly in the defense sector where the workforce is aging.

Research and Development

Manufacturing research and development is literally the core of an innovation machine that this Nation's economic engine is founded upon. Specifically, 70 percent of industrial R&D is performed by manufacturing-based companies, and the bulk of that R&D is applicable to manufacturing processes and procedures. This R&D results in the application of new technologies, new materials, and overall increased productivity within the manufacturing processes. All of these advances can make U.S. manufacturing more competitive within the global market, but only if the results of the R&D stay in the United States and add to the GDP for a significant period.

The Federal government has a role in the determination of R&D priorities, development of R&D clusters, investments for national security, and leveraging/ incentivizing private industry investment. A crucial need at the macro level is the planning and management of a collaborative and highly connected research enterprise which spans large and small businesses, academia, and government research laboratories. Recent studies of best in class foreign R&D strategies have concluded that developing regional "clusters" of specialized R&D partners provide the most effective model for government, academic, and industry innovation, and increase the probability of transition to domestic manufacturing capabilities. These clusters also offer the highest leveraging potential for government investment and have proven to drive associated capital investment in regional facilities and infrastructure.

Strategic Capabilities for National Security

One of the most critical balancing acts within the industrial policy domain is between open market competition and the creation or subsidizing of a domestic industrial capability. Industrial capabilities in manufacturing processes, raw materials, components, and technologies are disappearing from the United States every day in the form of off-shoring, business failures, supplier mergers, material shortages, global environmental restrictions, and lack of demand. In some cases, disappearing domestic capabilities can be replaced with overseas suppliers, but this is not possible for defense-essential capabilities, where access to domestic sources is a national security requirement. The current DoD industrial policy is to rely on market forces (competition) to create, shape, and sustain the industrial, manufacturing, and technological capabilities necessary to provide our fighting forces with systems that can engage and win full-spectrum warfare. However, when absolutely necessary, DoD will intervene to create and/or sustain competition, innovation, and essential industrial capabilities. If intervention is warranted, DoD can use mechanisms such as direct investment in supplier infrastructure, leveraging R&D investments, procurement assistance, purchase commitments, or collaboration with other Federal agencies to drive growth in domestic vendor demand.

Another critical issue is the need for steady, long-term access to affordable raw materials.

(Continued on Page 19)

Legal Insights

The Tanker Saga: Controversy at an End?

Introduction

The global military supremacy of the United States rests primarily on its ability to put "boots on the ground" and obtain ordinance on targets anywhere in the world within a very short time period. This mobility is predicated on the ability of an aircraft to receive fuel on the go or to refuel in mid-air by a refueling tanker aircraft. The United States Air Force's (USAF) current refueling tankers, the Boeing-built KC-135 and KC-10, were built in the Eisenhower era. A handful of failures and deaths in the 1990s and the early 2000s raised public awareness of aircraft degradation and related maintenance costs. On February 24, 2011, USAF announced that it had selected the Boeing Company's bid to provide the first batch of new air refueling tankers, dubbed the KC-X, rather than the bid of its chief rival, the European Aeronautic Defense and Space Company (EADS). Given the tumultuous, adversarial, and controversial decade-long saga to replace the U.S. military's four hundred plus aging refueling tankers, many procurement insiders are surprised that EADS has not challenged the award. This article will briefly summarize the decade of leases, bids, challenges, politics, and scandals surrounding this procurement, and highlight some of the more salient controversies that occurred along the way.

The Lease (2001 – 2003)

Boeing made an unsolicited offer to lease 100 Boeing 767-based fueling tankers to the USAF for $26 billion in 2001. In November 2001, the Undersecretary of Defense for Acquisition, Trade, and Logistics and the Undersecretary of Defense/ Chief Financial Officer established and chaired a leasing panel for the purchase, and in May 2003, the Secretary of Defense approved the leasing proposal. The lease was included in the fine print of the 2002 defense authorization bill. The lease was added by former Senator Ted Stevens (R-AK) in a closed session after the bill had passed both chambers, avoiding both the legislative authorization and appropriation procedures. The lease was shepherded through the legislative process by Ted Stevens as a way to move tankers into operation quickly and to avoid the years of bidding, evaluation, and production. This leasing method is how private airlines replenish their fleets in response to market needs. USAF's choice to pursue this "commercial" approach conflicted with the different set of rules that apply to the military and government procurement and expenditures. This mismatch, the application of a commercial technique to a military procurement, contributed to the waste (or corporate handout) of $6 billion. The Office of Management and Budget (OMB) estimated the cost of outright purchase of the aircraft contained in the lease to be $20 billion, creating a $6 billion surplus at the lease price of $26 billion.[1]

The Lease Backlash (2003 – 2004)

Senator John McCain (R-AZ) interpreted the lease as a corporate handout and aggressively investigated it as such. McCain had the weight of the Airland Subcommittee of the Senate Armed Services Committee behind him and it fit into his political person as an opponent of political "pork barrel" spending. He alleged a significant and coordinated lobbying effort by USAF and politicians that benefited from political donations from Boeing to deliver this surplus as a "bailout" to Boeing as its orders for new 767s was declining rapidly in the aftermath of September 11.[2]

(Continued on Page 12)

[1] Harris, Shane, "Own The Sky" Washingtonian.com, November 2010, http://www.washingtonian.com/print/articles/6/0/17244.html.
[2] Smith, R. Jeffrey, "Air Force Pitch for Boeing Detailed: E-mails Show Pressure by Roche" *Washington Post*, November 20, 2004, http://www.washingtonpost.com/wp-dyn/articles/A63815-2004Nov19.html.

Legal Insights *(Cont. from 11)*

McCain released several internal Pentagon communications supporting his campaign against the lease as a product of corporate-political-military collusion. These communications revealed that James G. Roche, USAF Secretary at the time, pushed for the lease. This put pressure on Boeing lobbyists to quiet dissenting voices in DoD and on military costs analysts, who noted the high price for the lease while publicly and privately promoting the Boeing tankers and dismissing a competing offer from Airbus.[3]

An investigation by DoD Inspector General Joseph E. Schmitz resulted in a March 2004 report that held that USAF "used an inappropriate procurement strategy and demonstrated neither best business practices nor prudent acquisition procedures to provide sufficient accountability for the expenditure…" and that "five statutory provisions that have not yet been satisfied."[4] The report further held that by inappropriately proceeding with a commercial lease with a fixed price and incorrectly treating the tankers as "commercial items" for procurement purposes, USAF did not have appropriate market data to produce a market price for the tankers. Furthermore, according to the report, USAF improperly relied on a wide range of inappropriate and insufficient data to develop accurate development, modification, and logistic price figures.[5] The inability to properly price led to systematic overpricing, allowing the contractor (Boeing) to retain any savings beyond the fixed-price agreed upon. Hence, the $6 billion overcharge. This also led to an expedited approach that did not fully and properly establish engineering, operational, or testing requirements necessary to ensure the long-term viability of the tankers eventually provided pursuant to the lease.[6] While the report did not explicitly recommend cancellation of the lease, it recommended either replacing the lease program with a competition or allowing USAF to proceed after curing the contracting and acquisition issues it identified, effectively dooming the lease.

The DOD IG's report did not kill the lease outright, but the fallout was significant. Secretary of Defense Donald Rumsfeld deferred a decision on the tanker in May 2004, and Congress cancelled the lease in October of that year. As a result, Boeing paid $615 million in fines. Furthermore, Boeing's Chief Executive Officer, Phil Condit, resigned. Boeing Chief Financial Officer, Michael Sears, went to prison for four months after pleading guilty to violating an ethics law covering employment negotiations with defense officials. One of the officials, Darleen Druyun, the second-ranking civilian in USAF procurement, went to prison for nine months for negotiating terms of employment at Boeing with Sears in October 2002 for herself as well as her son and daughter-in-law. She also pled guilty to overpricing the lease as a "parting gift" to Boeing. In June 2005, the Senate Armed Service Committee urged the DOD OIG to un-redact the identities of high-ranking White House, Pentagon, and Boeing officials from his report. They claimed the story had not been completely told and that the "lone gunman" theory of blaming the bulk of the wrongdoing on Darleen Druyun was letting too many other guilty parties off the hook.[7]

The Competition, First Round (2005 – 2008)

In September 2005, after a new competition was announced to provide the first 179 tankers, Northrop Grumman partnered with EADS, the parent company of Airbus, to bid against Boeing. McCain's insistence on fairness and transparency during the lease

(Continued on Page 13)

[3] Ibid.
[4] Department of Defense, Office of the Inspector General, Acquisition of the Boeing KC-767A Tanker Aircraft, D-2004-64, (March 2004) I, http://www.dodig.mil/audit/reports/fy04/04-064.pdf.
[5] Department of Defense, Office of the Inspector General, Acquisition of the Boeing KC-767A Tanker Aircraft, D-2004-64, (March 2004), ii-v, http://www.dodig.mil/audit/reports/fy04/04-064.pdf.
[6] Department of Defense, Office of the Inspector General, Acquisition of the Boeing KC-767A Tanker Aircraft, D-2004-64, (March 2004), iii-v, http://www.dodig.mil/audit/reports/fy04/04-064.pdf.
[7] Mike Allen, "Details on Boeing Deal Sought," *Washington Post*, (June 8, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/06/07/AR2005060701751.html.

Legal Insights *(Cont. from 12)*

debacle actually changed the way the competition was judged.[8] In December 2006, in a letter to Pentagon officials, McCain encouraged them to not consider the effect of penalties arising from a Boeing-Airbus World Trade Organization (WTO) dispute over subsidies. He also recommended that they award points for cargo space on a pro-rated basis rather than simply qualifying bidders based on their achievement of a minimum cargo amount.[9] Boeing ended up on the better side of that trade dispute, with the WTO finding in September of 2009 that European countries had contributed billions in illegal subsidies to Airbus. However, they ended up on the losing side for future bidding wars, as any resultant penalties on Airbus could not be considered per the rules in this round of bidding.

McCain's primary focus (also joined at this point by Alabama Senator Richard Shelby) in the admonishments he made to the Pentagon regarding the tanker bids was to comprehensively focus on and therefore evaluate the bids based on the value to the tax payer, not the absolute lowest cost. The December 2006 letter also contained McCain's recommendation that the bids be evaluated based on a capabilities-based, best-value approach rather than on the previously planned emphasis on lowest price. The January 2007 request for proposals (RFP) revealed that the Pentagon had heeded McCain's warning: they were indeed pursuing a "best value" approach, evaluating each bid on the value to the taxpayer. Northrop-EADS was prepared to withdraw from the competition if this approach was not adopted; they wanted due credit to be given to the fact that the higher fuel burn rate (higher cost) they had to include pursuant to the RFP's model corresponded to their larger aircraft's greater cargo (fuel for refueling) capacity.

On February 29, 2008, USAF announced its decision to buy 179 tankers from Northrop-EADS over time for an estimated $35 billion. Northrop-EADS planned on building most of the tankers in Mobile, AL, repurposing existing Airbus A330s into tankers at that site. The Boeing bid would have created 9,000 jobs and supported 35,000 whereas Northrop-EADS would have created 2,000 and supported 25,000.[11] However, the Northrop-EADS bid represented a savings of $6.2 billion. The Northrop-EADS tanker was larger and could carry more fuel and payload. It was also less of a production risk because the plane already existed in the Airbus A330; similar, repurposed A330s were successfully operating as refueling tankers in other national militaries.

Boeing Challenge of the Northrop-EADS Victory (2008)

Following Northrop-EADS' victory in February 2008, Boeing filed a protest with the Government Accountability Office (GAO) 11 days after the award. GAO supported Boeing's protest and, in June 2008, released a report detailing errors in the decision to give the bid to Northrop-EADS. The report contained non-binding recommendations to re-open the competition to re-evaluate the bids properly. Specifically, GAO found that USAF had engaged in "misleading and unequal discussions with Boeing."[12] According to the report, USAF told Boeing its bid had met a requirement. As it turns out, it was determined that Boeing had in fact not met the determination, although USAF provided more accurate and up-to-date information on the same requirement to Northrop-EADS. GAO also found that USAF had not strictly followed the scoring process and had improperly awarded Northrop points for exceeding technical requirements in a different order of priority than

(Continued on Page 14)

[8] Benjamin H. Friedman,, "Airbus, Alabama, Boeing, and McCain," Cato @ Liberty, (March 13, 2008), http://www.cato-at-liberty.org/airbus-alabama-boeing-and-mccain/.
[9] Ibid.
[10] David Freddosso,, "A Good Deal of Credit to McCain for Stopping a Bad Deal," National Review Online, (March 10, 2008), http://www.nationalreview.com/articles/223873/good-deal-credit-mccain-stopping-bad-deal/david-freddoso.
[11] Ibid.
[12] Government Accountability Office, "Statement Regarding the Bid Protest Decision Resolving the Aerial Refueling Tanker Protest by The Boeing Company," (June 18, 2008), 2, http://www.wired.com/images_blogs/dangerroom/files/gao_protest.pdf.

Legal Insights *(Cont. from 13)*

listed in the RFP.[13] Most importantly, USAF used the fact that the Northrop-EADS tanker exceeded a refueling performance parameter more than the Boeing tanker as a "key discriminator." In fact, consideration for exceeding performance parameters was explicitly disallowed in the RFP.[14]

A draft of new bidding rules was released in August 2008. Boeing responded by claiming it needed more time to assure that its bid complied with the new draft rules. The Pentagon canceled the tanker competition in September 2008. This effectively "kicked the can" to the next administration, or, as Secretary of Defense Gates stated at the time, provided a "cooling off period" for all parties involved.[15] It is worth noting that the challenge was successful for Boeing in two ways: 1) they increased their chances of eventually winning and filling this contract, and 2) continued to maintain the aging tanker fleet, comprised entirely of Boeing aircraft.

The Competition, Second Round (2009 – 2011)

The third attempt by USAF to replace their aging refueling aircraft took the form of a second competitive process: a new RFP was issued by USAF in September 2009. This second RFP represented a fundamental change to a "lowest price, technically acceptable" standard. This removed all subjective interpretation from the evaluation process and required reviewers to determine two facts in isolation: does the bid meet the minimum technical specifications required and, if so, at what price per aircraft? In response to the lease backlash from 2004 and Boeing's successful protest in 2008, by removing practically all opportunities for subjective evaluation, the second RFP was in fact a competition based solely on price.

A corollary to this change was the provision that if one bidder bid a price that was one percent or more less than competitors, USAF would simply buy the cheaper tanker.[16] To illustrate the change between rounds of competition, the first RFP contained only 37 mandatory, "go to war on day 1" requirements and 771 optional requirements. In contrast, the second RFP contained 373 mandatory requirements and 93 optional requirements, requirements that would not even be considered if the price differed by one percent or more.

Northrop Grumman viewed this drastic change from the value-based competition in the previous round (that it won in partnership with EADS) as a sign that the domestic political forces arrayed in support of Boeing had trumped those arrayed in favor of the Northrop-EADS partnership. Consequently, in March 2010, Northrop Grumman withdrew from the partnership with EADS as well as the competition after the final RFP was not changed to reflect their concerns.[17] Their advantage in delivering more fuel and materiel was rendered moot. EADS soldiered on, believing that the opportunity to gain a foothold in the U.S. aviation market was too immense to surrender. EADS also believed that its better tanker, quicker production time, and political backing from the southern States in which it proposed to build these tankers gave it a real chance to overcome the existing support for Boeing.

Initial bids were submitted in July 2010 and final bids in February 2011. The KC-X contract was awarded to Boeing on February 24, 2011. According to USAF, they were a "clear winner" based on price alone; the optional 93 requirements were not considered. As of March 2011, EADS North America's chairman has said they have no plans to appeal the award.[18]

(Continued on Page 20)

[13] Ibid.
[14] Ibid.
[15] Shane Harris,, "Own The Sky" Washingtonian.com, (November 2010), http://www.washingtonian.com/print/articles/6/0/17244.html.
[16] "The USAF's KC-X Aerial Tanker RFP," *Defense Industry Daily*, (March 13, 2011), http://www.defenseindustrydaily.com/the-usafs-kcx-aerial-tanker-rfp-03009/.
[17] Spencer Ackerman, "Corporate Crime, Corroding Planes: The Inside Story of the Air Force's Tanker Mess," Wired.com/Danger Room, (November 2, 2010), http://www.wired.com/dangerroom/2010/11/corporate-crime-corroding-planes-the-inside-story-of-the-air-forces-tanker-mess/.
[18] http://www.defenseindustrydaily.com/the-usafs-kcx-aerial-tanker-rfp-03009/.

GITA's GIS for Oil & Gas Pipeline Conference

October 24-27, 2011

Marriott Westchase Hotel
Houston, TX

www.gita.org/oilgas

5th Annual Security Analysis and Risk Management Conference

"Security Risk 10 Years After 9/11:
How Far Have We Come and What Lies Ahead?"

Tuesday, September 13, 2011 to Thursday, September 15, 2011

Including presentations and panel discussions on:

- Community Risk
- Critical Infrastructure Risk
- Cybersecurity Risk
- Public Policy for Risk Management
- Risk Education and Training
- Risk Management Standards
- Security Risk Methodologies and Practices

Conference and Reception co-hosted by CIP/HS and SARMA

at

George Mason University - Arlington Campus
Founders Hall
3351 Fairfax Dr.
Arlington, VA 22201

Please check our websites at http://cip.gmu.edu/ and http://sarma.org/ for regular updates on keynote speakers, presentations and panels, sponsors, exhibitors and more.

The Tenth Workshop on Economics of Information Security (WEIS 2011)

Tuesday, June 14, 2011 to Wednesday, June 15, 2011

at

The Mason Inn Conference Center and Hotel
4352 Mason Pond Drive
Fairfax, Virginia 22030

Registration is open!!!

Early Bird Registration fees are as follows (additional $50 after June 1st):
Academic/government/post-doc -- $500
Student -- $200
Industry -- $600

For additional information and to register for this event, please visit:
http://www.regonline.com/builder/site/Default.aspx?EventID=960652.

Workshop on Cybersecurity Incentives

June 16, 2011

Mason Inn Conference Center and Hotel
George Mason University, Fairfax, VA

Workshop Objectives

This workshop brings together researchers, economists, policymakers and practitioners to discuss the technical models and incentives that could lead to an increase in the adoption of more secure cyber capabilities. The workshop is aimed at:

- ✓ Promoting the prioritization of security in risk management decision making
- ✓ Improving the understanding institutional designs which create incentives for security
- ✓ Exploring implementable cybersecurity governance mechanisms at the enterprise and national levels

Other presenters

Sean Barnum, MITRE Corp.
L. Jean Camp, PhD, Indiana Univ.
Joe Jarzombek, DHS
Brent Rowe, RTI International
Robert Sloan, PhD, Univ. of Illinois-Chicago
Richard Warner, JD, Chicago-Kent Law School

Workshop Co-Chairs

Daniel E. Arista, SRC, Inc.
Timothy P. Clancy, J.D., George Mason University

Keynote Speaker

Joel Brenner, JD, PhD
Of Counsel, Cooley, LLP

Before joining Cooley, Mr. Brenner held notable appointments such as the Senior Counsel at the National Security Agency, U.S. Counterintelligence Executive, Office of the Director of National Intelligence, Inspector General at the National Security Agency, and as a Prosecutor in the Justice Department's Antitrust Division. He holds a JD from the Harvard Law School, a PhD from the London School of Economics, and a BA from the University of Wisconsin – Madison

Opening Remarks

Bruce Schneier
Chief Technology Officer, BT

Mr. Schneier is the founder and CTO of BT Counterpane, formerly Counterpane Internet Security, Inc. As the inventor of outsourced security monitoring and the foremost authority on effective mitigation of emerging IT threats, Schneier is the author of eight books on the subject, and one of his earlier books, Applied Cryptography, is the seminal work in its field. He writes the free email newsletter Crypto-Gram, which has over 70,000 readers. He received his master's degree in computer science from the American University in Washington, DC.

The Workshop on Cybersecurity Incentives (WoCI) will discuss the history, present, and future of societal mechanisms and institutional designs that leverage incentives to bring an acceptable balance between security and other priorities in cyberspace. The agenda will focus on illustrating cyberspace as an ecosystem of actors and discuss their roles and responsibilities, and the dynamics of their interaction and interconnectivity. Scholarship in law, economics and other fields within the behavioral sciences inform stakeholders about how markets, incentives and legal rules affect each other and shed light on determinations of liability and responsibility. This is considered essential to achieving efficient accountability and a sound public-private order in cyberspace. Considerations of what is technologically possible and feasible will be included. Ongoing debate and research in this area will be presented in practical terms allowing for participants to immediately realize implementable options for governing cybersecurity at the enterprise and national levels. The workshop will discuss the legal, economic and technological facets of the topics presented.

Presented by
GEORGE MASON UNIVERSITY
Center for Infrastructure Protection and Homeland Security

Presented by
SRC

Promotional Partner
AFEI

For more details on the workshop visit
http://cip.gmu.edu/woci2011.html

Sector Overview *(Cont. from 6)*

wider DIB community. DoD is also working to increase the DIB information sharing environment at the local level and to integrate DIB owners and operators into information mechanisms at State and local fusion centers.

DIB and Cybersecurity

In addition to JBP, DoD has significant efforts underway to increase DIB cybersecurity. Through the 2007 DIB Cyber Security/Information Assurance Pilot, DoD explored a comprehensive approach for protecting unclassified but sensitive DoD information transiting or residing on unclassified DIB information systems and networks. This effort involves sharing information on cyber threats, providing expert advice and assistance, cooperating on incident responses, and evaluating the damage of cyber intrusion. Currently, 36 companies participate in the initial pilot, which has resulted in greater shared understanding of advanced cyber threats, increased information sharing on cyber incidents and the potential impact of those incidents on DoD capabilities, and overall increased cybersecurity capabilities. DoD's goal is to expand the current pilot to all cleared defense contractors and eventually to other critical, uncleared DIB partners. The Department recently approved $113 million for the period between 2011-2016 to convert the DIB Cyber Security/Information Assurance Pilot to program status. DIB cybersecurity remains a top priority for DoD, and we expect to continue to build on current efforts to find innovative ways to extend DoD cybersecurity to our industry partners that provide critical support to DoD's mission.

Additionally, DIB partners formed the Defense Security Information Exchange (DSIE) that acts as a DIB SCC Cyber Security standing committee. DSIE was formed using a trust model developed originally in the Network Security Information Exchanges (NSIE). In February 2008, DSIE was formalized under the DIB Sector Coordinating Council as the Cyber Sub-Council. The members use their trust relationships to share intelligence on cyber related attacks. This sharing has enabled the industry partners to quickly alert others of any ongoing incidents and share mitigation strategies for the protection of the DoD CIKR under their control. The DSIE now consists of over 55 member companies and 300 trusted cybersecurity engineers. In today's expanding and persistent threat environment, it is important to build on these successful sharing models to combat attackers. The success and the strength of the DSIE processes are due to the dedication of the individual members. Their commitment to this effort has been extraordinary. Through their continued support, they have made DSIE, their organization, what it is today.

Summary

DoD is committed to ensuring the security and resilience of the Defense Industrial Base. The foundation of the Sector's security is in understanding and sharing information, building protective partnerships, implementing long-term risk management programs, and maximizing efficient use of resources. DoD continues to engage the DIB SCC to identify priority concerns, share views on security-related issues, and ultimately increase DIB resilience. DIB private sector partners have indicated the desire to do more and share their expertise. Through joint efforts we can work to implement risk-based mitigation efforts that support DoD mission assurance. ❖

NDIA *(Cont. from 10)*

Sometimes, having domestic manufacturing capability is not enough, as in the case of secure access to raw materials. A U.S. industrial base can depend upon materials which are not readily available or affordable, causing additional cost, schedule, or failure. The Government Accountability Office[2] concluded that DoD lacks a consistent, department-wide framework to monitor its supplier base. This vulnerability is particularly salient for strategic materials such as titanium, cobalt, and rare earth materials, which have major applications in advanced weapons systems such as smart bombs, night-vision goggles, and radar. Today, China produces 97.3 percent of the world's supply of rare earth minerals; Russia produces 1.6 percent, while the United States produces only 1.1 percent.

A crucial tool for assessing the U.S. defense industrial base is visibility into the lower levels of the supply chain, at the second and third tier. Traditionally, DoD takes the responsibility for monitoring the capabilities and competitive viability of prime contractors, Original Equipment Manufacturers (OEM), and key first tier suppliers. The capabilities and viability of lower tier suppliers is monitored by the primes and OEMs, which have access to and contracts with these suppliers. The recent economic challenges have highlighted the dangers in not understanding these lower tiers, which are predominately small businesses and at most risk for failure from demand volatility or access to capital.

Manufacturing Workforce and Infrastructure

The manufacturing workforce has been shrinking over the past 40 years, as productivity increases have allowed manufacturing output to remain steady using fewer labor hours. However, in recent recessions, the drop in employment has been precipitous, with over 4.5 million manufacturing jobs lost in the past ten years. The reason for this large decrease has been the interaction of three forces: offshore manufacturing, increased productivity, and a decline in manufactured goods demand during the recession. Off-shoring is a response to lower foreign structure costs, and increased productivity is the natural competitive reaction to those costs. The only method of increasing employment in the manufacturing sector is to increase the demand, either domestically or through exports, and this requires new technology, either in terms of new products or, more often, advanced manufacturing. Advanced manufacturing technologies, particularly at the enterprise level, requires a workforce with special skills, such as familiarization with 3-D models, distributed supply chain interaction, and digital work instructions. These skills will be required in the near future in order for the United States to compete in either the domestic or export markets when there are no current government programs or leadership to drive this innovation into the workforce. ❖

[2] General Accountability Office, *DoD Assessments of Supplier-Base Availability for Future Defense Needs*, GAO-10-317R, (January 27, 2010).

DIB Challenges *(Cont. from 8)*

help save U.S. taxpayer dollars over time and reduce wear and tear on U.S. equipment. An increase in international sales will require both limiting the restrictions placed on the defense sector by the U.S. International Trade in Arms Regulations (ITAR), which are both time-consuming and confusing, and, in the case of America's closest allies, negotiating bilateral defense trade cooperation treaties to help facilitate easier market access. Reformed export control policies must preserve innovation as a commodity. While the concern that sensitive defense technologies may fall into the wrong hands without proper oversight is valid, the archaic ITAR regulations remain insufficient in today's globalizing defense market. ❖

Mackenzie Eaglen is Senior Policy Analyst for National Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.

Legal Insights *(Cont. from 14)*

Conclusion

Given a decade of rancorous, adversarial competition between Boeing and EADS over the provision of refueling the tanker aircraft and the importance of this contract to the worldwide aviation market, one must wonder why EADS is not protesting this most recent award. The simple response is that procurement officials have twice been burned badly, first when they attempted to remove the acquisition from the procurement process with a commercial lease and then again when they allowed subjective determinations of value to determine the winner in the first competition. In response to the criticism for lack of transparency and the use of subjective criteria, USAF framed the second round of competition to make it "protest-proof." They effectively made two completely objective determinations: that the proposed aircraft met minimum requirements and that one price was lower than another. Politics and profit were driving forces in this saga, and the fact that detractors from EADS and their political allies have yet to find fault on which to base a protest attests to the success of USAF in designing and executing a transparent and objective procurement. Only time will tell if the focus on price rather than value was worth the peace and quiet. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1